Polynomial Rings

R ring $\qquad x$ variable

$R[x] =$ Set of all polynomials with coefficients in R

$$= \left\{ a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; \begin{array}{l} n \in \mathbb{N} \\ a_i \in R \end{array} \right\}$$

Some observations:

1) If R is commutative, $R[x]$ is commutative

2) If R is integral domain, $R[x]$ is an integral domain.

Pf: Suppose $f(x)\,g(x) = 0$

If $f = 0$ or $g = 0$, then we are done.

Suppose $f \neq 0$ and $g \neq 0$.

Assume $\deg(f) = n \qquad f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$(a_n \neq 0)$

Assume $\deg(g) = m$ $\quad g(x) = b_0 + b_1 x + \cdots + b_m x^m$
$(b_m \neq 0)$

$$f(x)\, g(x) = a_n b_m X^{n+m} + \cdots + a_0 b_0$$

Since R is an integral domain $a_n b_m \neq 0$

$\Rightarrow f(x)\, g(x) \neq 0$ which is a contradiction.

3) If R is a field, we can divide in $R[x]$, i.e. given two polynomials f, g in $R[x]$, there exists quotient $q(x)$ & remainder $r(x)$ such that

$$f(x) = g(x)\, q(x) + r(x)$$

where $r(x) = 0$ or $\deg r < \deg g$

Pf: If $\deg f < \deg g$

then take $q = 0$
$r = f$

Assume that $\deg f \geq \deg g$

If $f(x)=0$, then $q=0$, $r=0$ works.

Assume that $f(x) \neq 0$.

Say $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ $\quad a_n \neq 0$

and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ $\quad b_m \neq 0$

Consider

$$f(x) - \left(\frac{a_n}{b_m} x^{n-m} \right) g(x)$$

$$= a_0' + a_1' x + \cdots + a_{n-1}' x^{n-1}$$

If $n-1 < m$ then stop otherwise proceed similarly.

After a finite number of steps, we have

$$f(x) - \underbrace{\left(\frac{a_n}{b_m} x^{n-m} + \cdots \right)}_{q(x)} g(x) = r(x)$$

Corollary: If I is an ideal of $R[x]$, where R is a field, then I is principal, i.e. $I = \langle f(x) \rangle$.

$$\langle f(x) \rangle = \{ f(x)\,g(x) \mid g(x) \in R[x] \}$$

Pf: Assume $I \neq 0$ and $I \neq R[x]$.

Choose a polynomial f in I such that $f \neq 0$ and f has smallest degree in I.

Then for any $g \in I$

$$\underbrace{g}_{\in I} = \underbrace{fq}_{\in I} + r \quad \Rightarrow r \in I$$

So, $r = 0$.

Let F be a field.

Let $F[x]$ denote the polynomial ring.

Defn: We say that a polynomial $f(x)$ $(\deg f \geq 1)$ $\in F[x]$ is irreducible if we cannot factor f, i.e. if $f(x) = g(x)\, h(x)$ then either g or h is a non-zero constant.

Examples: 1) Any degree 1 polynomial is irreducible.

2) x^2+1 is irreducible in $\mathbb{R}[x]$.

x^2+1 is not irreducible in $\mathbb{C}[x]$.

3) x^2-2 is irreducible in $\mathbb{Q}[x]$.

x^2-2 is not irreducible in $\mathbb{R}[x]$.

Lemma: If $f(x) \in F[x]$ is a degree 3 or degree 2 polynomial and $f(x)$ does not have a root in F, then $f(x)$ is irreducible.

Proof: Suppose $f(x)$ is not irreducible, then

$$f(x) = g(x)\, h(x)$$

where g or h has degree 1

So, $f(x) = (x-a)\, h(x)$ for some $a \in F$

$\Rightarrow$ $f(a) = 0$

This does not hold for higher degree polynomials.

Consider $(x^2+1)(x^2+2) = f(x)$
$\downarrow$
degree 4

irreducible in $\mathbb{Q}[x]$.

F field

$F[x]$ polynomial ring

$f(x) \in F[x]$

$\downarrow$

irreducible

Let I be an ideal of $F[x]$ generated by f, i.e. $I = \langle f(x) \rangle$.

Thm: $F[x]/I$ is a field.

Pf: Consider a coset $g(x) + I$, $g(x) \neq 0$. So $\deg g < \deg f$.

Take the ideal J in $F[x]$ generated by $g(x)$ and $f(x)$, i.e.,

$$J = \{ g(x)\, h_1(x) + f(x)\, h_2(x) \mid h_1, h_2 \in F[x] \}$$

We know that J is principal so,

$$J = \langle r(x) \rangle$$

$\Rightarrow \quad f(x) = r(x)\, r_1(x)$

but $f(x)$ is irreducible so, either

$f(x) = c\, r(x)$ c is a constant $(c \neq 0)$

or $r(x)$ is a constant (not zero)

If $r(x)$ is a non-zero constant

$\Rightarrow \quad J = F[x] = \langle 1 \rangle$

$\Rightarrow \quad 1 = g(x)\, h_1(x) + f(x) h_2(x)$ for some $h_1, h_2 \in F[x]$

$\Rightarrow \quad 1 = g(x)\, h_1(x)$ in $F[x]/I$.

If $f(x) = c\, r(x)$

$\Rightarrow \quad J = I$

$\Rightarrow \quad g(x) \in I \Rightarrow g(x)$ is zero in $F[x]/I$

$\downarrow$

contradiction.

Can we compute this field explicitly?

F field (char 0)

$F[x]$ polynomial ring

$f(x)$ irreducible polynomial

Suppose $f(\alpha) = 0$ for some $\alpha \in \mathbb{C}$

(α not necessarily in F)

Definition: We define $F[\alpha]$

$$= \left\{ a_0 + a_1\alpha + \cdots + a_n\alpha^n \,\middle|\, \begin{array}{l} a_i \in F \\ n \in \mathbb{N} \end{array} \right\}.$$

1) $F \subseteq F[\alpha]$

2) $F[\alpha] \subseteq \mathbb{C}$

3) $F[\alpha]$ is a subring of $\mathbb{C}$.

Thm: $F[\alpha]$ is a field.

Pf: Let us define a map

$\varphi_\alpha : F[x] \to F[\alpha]$ as follows.

$$g(x) \longmapsto g(\alpha)$$

φ_α is a ring homomorphism.

<u>Claim:</u> $\ker \varphi_\alpha = \langle f(x) \rangle$

<u>Pf:</u> If $\varphi_\alpha(g) = g(\alpha) = 0$, we want to show that $g(x)$ is a multiple of $f(x)$.

<u>Observation:</u> If $h(\alpha) = 0$ and $h(x)$ is non-zero, then $\deg h(x) \geq \deg f(x)$

Suppose not, then we consider the set of polynomials

$$S = \left\{ h(x) \in F[x] \;\middle|\; \begin{array}{l} h(\alpha) = 0,\ h \neq 0 \\ \deg h < \deg f \end{array} \right\}$$

S is non-empty, so we can choose a polynomial $r(x) \in S$ of smallest degree.

By division algorithm

$$f(x) = r(x)\, q(x) + r_1(x)$$

Put $x = \alpha$ $\quad f(\alpha) = r(\alpha)\, q(\alpha) + r_1(\alpha)$

$f(\alpha) = 0$, $r(\alpha) = 0$

$\Rightarrow r_1(\alpha) = 0$

$\Rightarrow r_1 = 0$, otherwise $r_1(x) \in S$ & $\deg r_1 < \deg r$
a contradiction.

$\Rightarrow f(x) = r(x)\, q(x)$

Since f is irreducible $\deg r = \deg f$
or r is a non-zero constant

$\downarrow$

Both give contradiction.

Finishing pf of the claim:

If $g(x) = 0$, we are done, else $\deg g \geq \deg f$

$g(x) = f(x)\, q(x) + r(x)$

Put $x = \alpha$ $\Rightarrow r(\alpha) = 0 \Rightarrow r = 0$

So, g is a multiple of f.

$\Rightarrow$ $\operatorname{Ker} \varphi_\alpha \subseteq \langle f(x) \rangle$

$\langle f(x) \rangle \subseteq \operatorname{Ker} \varphi_\alpha$ follows because

$f(\alpha) = 0$.

So, $\operatorname{Ker} \varphi_\alpha = \langle f(x) \rangle$

Image $\varphi_\alpha = F[\alpha]$

By first isomorphism theorem

$$F[x] / \langle f(x) \rangle \cong F[\alpha]$$

$\downarrow$

field

So, $F[\alpha]$ is a field.

Examples

Example: 1) Evaluation at a point

F field $\quad P_a : F[x] \longrightarrow F \qquad a \in F$

$$f(x) \longmapsto f(a)$$

$$\operatorname{Ker} P_a = \langle x-a \rangle$$

$$\text{Image} = F$$

$$F[x] \big/ \langle x-a \rangle \cong F$$

2) $P_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$

$$f(x) \longmapsto f(i) \qquad i^2 = -1$$

$$\operatorname{Ker} P_i = \langle x^2+1 \rangle$$

$$\text{Image } P_i = \mathbb{C}$$

$$\mathbb{R}[x] \big/ \langle x^2+1 \rangle \cong \mathbb{C} = \mathbb{R}[i]$$

3) $f(x) = x^2 - 2 \in \mathbb{Q}[x]$

$$\mathbb{Q}[x] / \langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}]$$